UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/753,727 | 01/03/2001 | Rosario Gennaro | RSW920000091US1 | 3760 |

7590 08/04/2004

Gerald R. Woods
IBM Corporation T81/503
P.O. Box 12195
Research Triangle Park, NC 27709

| EXAMINER | |
|---|---|
| HENNING, MATTHEW T | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | 3 |

DATE MAILED: 08/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/753,727 | GENNARO, ROSARIO | |
| | Examiner | Art Unit | |
| | Matthew T Henning | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *03 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☒ Claim(s) *4,6,16,18,28,30,42 and 44* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 01/03/2001.

## DETAILED ACTION

1. Claims 1-47 have been examined.

### *Title*

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: *Method, Apparatus, and Computer Program Product for Generating Pseudo-Random Bits.*

### *Priority*

3. No claim for priority has been made for this application.

4. The effective filing date for the subject matter defined in the pending claims in this application is January 03, 2001.

### *Information Disclosure Statement*

5. The information disclosure statement (IDS) submitted on 01/03/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

### *Drawings*

6. The drawings filed on 01/03/2001 are acceptable for examination proceedings.

### *Specification*

7. Applicant is reminded of the proper language and format for an abstract of the disclosure.

*The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract*

*on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.*

*The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.*

8. The abstract of the disclosure is objected to because

Line 2: The phrase "the present invention provides" can be implied and therefore must be removed.

Lines 9-11: The sentence "This generator...on the DLSE" compares the present invention to the prior art and therefore must be removed.

Correction is required. See MPEP § 608.01(b).

9. The disclosure is objected to because of the following informality. Page 18 Paragraph 3 recites that the modular multiplications required by the present invention are calculated by the formula (1.5 log x) where x is the number of bits in the exponent, but when applying this formula as an example the "log" operation is left out, which leads the reader to become confused about the required modular operations required by the present invention.

Appropriate correction is required.

***Claim Objections***

10. The applicant is reminded that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

11. Claims 4, 6, 16, 18, 28, 30, 42, and 44 are objected to because of the following informality:

Claims 4, 16, 28, and 42 Line 1 recites "is used an" which is grammatically incorrect. Appropriate correction is required.

Claims 6, 18, 30, and 44 are objected to by virtue of their dependencies.

***Claim Rejections - 35 USC § 102***

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

*A person shall be entitled to a patent unless –*

*(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*

13. Claims 13-22, 24-35, and 37-47 are rejected under 35 U.S.C. 102(b) as being anticipated by Patel et al ("An Efficient Discrete Log Pseudo Random Generator") hereinafter referred to as Patel.

14. Claim 13 recites a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value (See Patel Page 313 Section 5 Line 10); and means for generating an output sequence of pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12) using the provided input value

as input to a 1-way function (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i} \bmod p$ is one-way) wherein a length of the input value is substantially shorter than a length of the generated output sequence (See Patel Page 307 Problem 2).

15. Claim 14 recites that the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption (See Patel Page 307 Section 2.1).

16. Claim 15 recites that the 1-way function is modular exponentiation modulo a safe prime number (See Patel Page 313 Section 5 Line 10 and Page 307 Paragraph 6 Lines 7-8).

17. Claim 16 recites that the input value is used as an exponent of the modular exponentiation (See Patel Page 313 Section 5 Line 10).

18. Claim 17 recites that a base of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4).

19. Claim 18 recites that the length of the input value is 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and a length of the safe prime number is 1024 bits (See Patel Page 307 Lines 5-6).

20. Claim 19 recites that the length of the input value is at least 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and the length of the generated output sequence is at least 1024 bits (See Patel Abstract Lines 11-13 wherein n is the number of bits output by the generator prior to bit extraction as disclosed by Patel in Section 6).

21. Claim 20 recites means for selecting a subset of bits from the generated output sequence as a next sequential input value, wherein a length of the selected subset is identical to the length of the input value; and means for generating a next sequential output sequence of pseudo-random bits using the next sequential input value as input to the 1-way function, wherein a length of the next sequential output sequence is identical to the length of the generated output sequence (See Patel Section 7.1 Paragraph 2).

22. Claim 21 recites means for concatenating bits of the generated next sequential output sequence which are not selected by the means for selecting to the generated output sequence to form a longer output sequence of pseudo-random bits (See Patel Abstract and Section 7.1).

23. Claim 22 recites that the means for selecting the subset of bits comprises selecting a contiguous group of bits (See Patel Section 7.1 Line 8).

24. Claim 24 recites means for using the longer output sequence as input to an encryption operation (See Patel Page 305 Lines 15-17).

25. Claims 25-35 are rejected for the same reasons as claims 13-22 above.

26. Claim 37 is rejected for the same reasons as claim 24 above.

27. Claim 38 is rejected for the same reasons as claims 33 and 34 above, and further because Patel disclosed iterative bit generation (See Patel Section 7.1).

28. Claim 39 is rejected for the same reasons as claims 13 and claim 24 above.

29. Claims 40-47 are rejected for the same reasons as claims 14-21, and 24 above.

***Claim Rejections - 35 USC § 103***

30. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

31. Claims 23, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel as applied to claims 20 and 33 respectively above, and further in view of Schneier ("Applied Cryptography").

Patel disclosed selecting a set of bits from the output as the new input (See rejection of claim 20 above), but failed to disclose that the bits were selected in a non-contiguous manner.

Schneier teaches that in order to reach a maximal period for a pseudo-random bit generator, the feedback bits should be a primitive polynomial mod 2 (See Schneier Page 374 lines 9-20, and further shows an example of this type of feedback (See Schneier Page 375 Figure 16.4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the pseudo-random bit generator of Patel in order to provide primitive polynomial mod 2 feedback to the generator. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the longest period for the generator to ensure the most produced bits before cycling.

32. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Patel, and further in view of Schneier ("Applied Cryptography").

Patel disclosed inputting a seed and then generating pseudo-random bits through a one-way function, in which the seed contained less bits than the output (See rejection of claim 13 above), but Patel failed to disclose that this system was implemented in software. However, Patel did disclose that these pseudo-random bits were for encryption (See Patel Page 305 Lines 15-17).

Schneier teaches that any encryption algorithm can be implemented in software and that doing so helps with flexibility and portability, ease of use, and ease of upgrade (See Schneier Page 225 Paragraph 7 Lines 1-3). Schneier further teaches that software encryption programs are popular (See Schneier Page 225 Paragraph 8 Line 1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the pseudo-random number generator of Patel by implementing the generator in software. This would have been obvious because the ordinary person skilled in the art would have been motivated to improve the portability, ease of use, and ease of upgrade of the generator.

33. Claims 2-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Patel and Schneier as applied to claim 1 above, for the same reasons as claim 14-24 above.

***Conclusion***

34. Claims 1-47 have been rejected.

35. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Patel et al. (U.S. Patent Number 6,285,761) disclosed a pseudo-random bit generator based on the assumption known as "discrete logarithms with short exponents".

36. Please direct all inquiries concerning this communication to Matthew Henning whose telephone number is (703) 305-0713. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Matthew Henning
Assistant Examiner
Art Unit 2131